Temat: Zakładanie kont użytkowników. Tworzenie grup.

Ogólny cel lekcji: Celem lekcji jest wprowadzenie uczniów do podstaw zarządzania kontami użytkowników i grup w systemach Windows. Uczestnicy zrozumieją znaczenie zarządzania dostępem do zasobów i bezpieczeństwa poprzez skupienie się na określaniu przynależności użytkowników do grup domeny oraz poznają różne strategie tworzenia grup.

Cele szczegółowe: Po zakończeniu lekcji uczestnicy powinni:

1. Zrozumieć, że zarządzanie kontami użytkowników, grup oraz kontami komputerów jest istotne dla zapewnienia bezpieczeństwa i efektywnego dostępu do zasobów w systemach Windows.

2. Rozpoznać i wyjaśnić różnicę między kontami użytkowników a kontami komputerów oraz zrozumieć rolę kont grupowych w organizacji dostępu.

3. Zdobyć wiedzę na temat struktury kontenerów i katalogu Active Directory oraz jak jest ona związana z zarządzaniem kontami użytkowników i grup.

4. Nauczyć się procesu tworzenia kont użytkowników i grup w środowisku lokalnym oraz na kontrolerze domeny.

5. Rozróżnić różnice między tworzeniem kont w środowisku lokalnym a w kontrolerze domeny oraz zrozumieć wpływ zarządzania na poziomie domeny.

6. Zdobyć wiedzę na temat podstawowych parametrów kont użytkowników i grup oraz ich znaczenia dla dostępu do zasobów.

7. Zrozumieć znaczenie zachowania bezpieczeństwa w kontekście operacji na hasłach i danych użytkowników.

8. Rozpoznać rolę organizacji w grupach jako narzędzia do uporządkowanego zarządzania dostępem do zasobów.

9. Zdobyć ogólną wiedzę na temat dostępnych narzędzi do zarządzania kontami użytkowników i grup, takich jak "Zarządzanie komputerem" i "Użytkownicy i komputery usługi Active Directory".

10. Zrozumieć zastosowanie narzędzia DSGET jako rozwiązania dla określania przynależności użytkowników do grup w usłudze Active Directory.

11. Prawidłowo interpretować wyniki polecenia DSGET, aby zrozumieć, do których grup należy użytkownik w skomplikowanych strukturach grupowych.

12. Zrozumieć, że narzędzie DSGET jest przykładem praktycznego rozwiązania w zarządzaniu dostępem, wspierającym skomplikowane struktury grupowe w organizacji.

13. Zrozumieć znaczenie strategii tworzenia grup w kontekście zarządzania dostępem do zasobów w sieci oraz ich roli w organizacji dostępu.

14. Wyjaśnić strategię A L P (Account, Local, Permissions) oraz zrozumieć, jak ta metoda nadawania uprawnień działa.

15. Zrozumieć zalety i ograniczenia strategii A L P w zakresie zarządzania dostępem na poziomie lokalnym.

16. Znać strategię A G DL P (Account, Global, Domain Local, Permissions) i umieć zastosować ją w zarządzaniu dostępem na poziomie domenowym.

17. Zrozumieć, jak hierarchia grup globalnych i grup domenowych lokalnych wpływa na strategię A G DL P.

18. Zrozumieć koncepcję i znaczenie strategii A G U DL P (Account, Global, Universal, Domain Local, Permissions) w kontekście wielodomenowych środowisk.

19. Porównać strategię A G DL P i strategię A G U DL P, rozumiejąc, w jakich przypadkach zastosowanie każdej z nich jest właściwe.

20. Zrozumieć znaczenie planowania i projektowania struktury grup dla efektywnego zarządzania dostępem do zasobów.

21. Rozumieć, jak każda z strategii wpływa na hierarchię uprawnień i dostęp do zasobów w kontekście sieci.

22. Rozpoznać praktyczne przykłady zastosowania każdej strategii w celu zapewnienia bezpieczeństwa i efektywnego zarządzania dostępem do zasobów.

Podsumowanie: Lekcja skupia się na wprowadzeniu uczniów w podstawy zarządzania kontami użytkowników i grup w systemach operacyjnych Windows oraz na zrozumieniu roli tych kont w organizacji dostępu do zasobów i bezpieczeństwa. Dodatkowo omawiane są strategie tworzenia grup w kontekście zarządzania dostępem, co pozwala uczestnikom zrozumieć różne podejścia do skutecznego zarządzania dostępem użytkowników w sieci.

A. Zarządzanie kontami użytkowników i grup

W systemach operacyjnych Windows, zarządzanie kontami użytkowników, grupami oraz kontami komputerów odgrywa kluczową rolę w kontroli dostępu do zasobów i w zachowaniu bezpieczeństwa. W różnych wersjach systemów Windows istnieją pewne różnice w mechanizmach zarządzania tymi kontami.

a. Konta użytkowników

Konta użytkowników reprezentują osoby korzystające z systemu. W systemie Windows można tworzyć, edytować oraz usuwać konta użytkowników. Umożliwiają one dostęp do zasobów systemowych i aplikacji.

Tworzenie konta użytkownika:

1. **Windows Server 2016, 2019, 2022:** Otwórz "Zarządzanie komputerem", a następnie znajdź "Użytkownicy i grupy lokalne" Wybierz Użytkownicy prawoklik Nowy użytkownik…
2. **Dodaj nowego użytkownika**, podając niezbędne informacje, takie jak nazwa użytkownika, hasło.
3. Zamknij.
4. Tworzenie konta użytkownika za pomocą wiersza poleceń (CMD):

```
net user [nazwa użytkownika] [hasło] /add
```

b. Zarządzanie grupami

Grupy służą do organizowania użytkowników w logiczne jednostki, ułatwiając zarządzanie dostępem do zasobów.

1. **Tworzenie grup:**

- Wskazówki są podobne do tworzenia konta użytkownika, ale wybieramy "Grupy" zamiast "Użytkownicy".
- Tworzenie grupy za pomocą wiersza poleceń (CMD):

```
net localgroup [nazwa grupy] /add
```

2. **Dodawanie użytkowników do grup:**

- Edytując grupę, możemy dodać użytkowników z dostępem do wspólnych zasobów.
- Dodawanie użytkowników do grupy za pomocą wiersza poleceń (CMD):

```
net localgroup [nazwa grupy] [nazwa użytkownika] /add
```

B. Tworzenie konta na kontrolerze domeny

Gdy korzystasz z kontrolera domeny w środowisku Windows, zarządzanie kontami użytkowników ma pewne różnice w porównaniu do zarządzania kontami na lokalnym komputerze.

a) Aby utworzyć konto grupy na kontrolerze domeny w środowisku graficznym, wykonaj poniższe kroki:

1. Zaloguj się do kontrolera domeny:

- Zaloguj się na kontrolerze domeny za pomocą konta administratora domeny lub konta, które ma uprawnienia do tworzenia kont grupy.

2. Otwórz konsolę Użytkownicy i komputery usługi Active Directory:

- W Windows Server 2016, 2019, 2022: Wyszukaj w menu "Start" i "Narzędzia Administracyjne systemu Windows" wybierz "Użytkownicy i komputery usługi Active Directory (Active Directory Users and Computers)".

3. Wybierz domenę:

- W konsoli "Użytkownicy i komputery usługi Active Directory (Active Directory Users and Computers)" kliknij prawym przyciskiem myszy na "Users" w drzewie konsoli po lewej stronie i wybierz "Nowy" > "Grupa".

4. Podaj informacje o grupie: Postępuj zgodnie z kreatorami tworzenia nowej grupy:

- Podaj nazwę i opis grupy.
- Określ zakres grupy (np. globalny, uniwersalny, lokalny).
- Określ typ grupy (np. zabezpieczenia, dystrybucja).

5. Zakończ tworzenie:

- Po uzupełnieniu wszystkich informacji, zakończ proces tworzenia konta grupy.

Konto grupy zostanie teraz utworzone w domenie, a będziesz mógł zarządzać jej członkami, uprawnieniami i dostępem do zasobów w obrębie całej domeny.

Zarządzanie kontami grupy w kontrolerze domeny jest ważne dla bezpieczeństwa i dostępu do zasobów w sieci. Pamiętaj, że nadanie odpowiednich uprawnień oraz zrozumienie struktury uprawnień grupy są kluczowe dla skutecznego zarządzania siecią.

b) Utworzenie konta użytkownika na kontrolerze domeny w środowisku graficznym:

6. Zaloguj się do kontrolera domeny:

- Zaloguj się na kontrolerze domeny za pomocą konta administratora domeny lub konta, które ma uprawnienia do tworzenia kont użytkowników.

7. Otwórz konsolę Użytkownicy i komputery usługi Active Directory:

- W Windows Server 2016, 2019, 2022: Wyszukaj w menu "Start" i "Narzędzia Administracyjne systemu Windows" wybierz "Użytkownicy i komputery usługi Active Directory (Active Directory Users and Computers)".

8. Wybierz domenę:

- W konsoli "Użytkownicy i komputery usługi Active Directory (Active Directory Users and Computers)" kliknij prawym przyciskiem myszy na "Users" w drzewie konsoli po lewej stronie i wybierz "Nowy" > "Użytkownik".

9. Podaj informacje o użytkowniku. Postępuj zgodnie z kreatorami tworzenia nowego użytkownika:

- Podaj imię, nazwisko i nazwę użytkownika.
- Wybierz hasło dla użytkownika (lub pozostaw pole puste, jeśli zależy Ci na wymuszeniu zmiany hasła po pierwszym logowaniu).
- Określ, czy użytkownik musi zmienić hasło przy następnym logowaniu.
- Określ grupy, do których ma należeć użytkownik (na przykład grupa użytkowników, administratorów itp.).

10. Zakończ tworzenie:

- Po uzupełnieniu wszystkich informacji, zakończ proces tworzenia konta użytkownika.

Konto użytkownika zostanie teraz utworzone w domenie, a użytkownik będzie mógł się zalogować na dowolnym komputerze w tej domenie.

Warto pamiętać, że zarządzanie kontami użytkowników w kontrolerze domeny ma większy wpływ na całe środowisko, ponieważ konta użytkowników będą miały dostęp do zasobów i usług w obrębie całej domeny. Dlatego ważne jest, aby dokładnie zrozumieć proces tworzenia i zarządzania kontami użytkowników w takim środowisku.

c) Aby utworzyć konto grupy na kontrolerze domeny za pomocą wiersza poleceń (CMD) i narzędzia dsadd:

1. **Otwórz wiersz poleceń**: Kliknij przycisk "Start", wpisz "cmd" i naciśnij Enter, aby otworzyć Wiersz Poleceń.
2. **Tworzenie konta grupy na kontrolerze domeny**: Użyj poniższego polecenia, aby utworzyć konto grupy:

```
dsadd group "CN=Nazwa Grupy,OU=OU_Nazwa,DC=Nazwa_Domeny,DC=pl" -secgrp yes -scope g
```

Gdzie:

"CN=Nazwa Grupy,OU=OU_Nazwa,DC=Nazwa_Domeny,DC=pl" to ścieżka do miejsca, gdzie chcesz dodać grupę.

-secgrp yes oznacza, że jest to grupa zabezpieczeń.

-scope g definiuje zakres grupy jako globalny.

Przykład:

```
dsadd group "CN=Sales Team,OU=Groups,DC=example,DC=com" -secgrp yes -scope g
```

Takie polecenie utworzy grupę "Sales Team" w organizacyjnej jednostce "Groups" na kontrolerze domeny o domenie "example.com".

Pamiętaj, że zarządzanie kontami grupy i użytkownika za pomocą wiersza poleceń wymaga odpowiednich uprawnień. Warto również pamiętać o bezpieczeństwie, szczególnie w przypadku operacji na hasłach i danych użytkowników.

d) Aby utworzyć konto użytkownika na kontrolerze domeny za pomocą wiersza poleceń (CMD) na kontrolerze domeny i narzędzia dsadd:

3. **Otwórz wiersz poleceń:** Kliknij przycisk "Start", wpisz "cmd" i naciśnij Enter, aby otworzyć Wiersz Poleceń.
4. **Tworzenie konta użytkownika na kontrolerze domeny:**

```
dsadd user "CN=Nazwa Użytkownika,OU=OU_Nazwa,DC=Nazwa_Domeny,DC=pl" -samid NazwaUzytkownika -pwd HasloUzytkownika -mustchpwd yes -memberof "CN=Nazwa Grupy,OU=OU_Nazwa,DC=Nazwa_Domeny,DC=pl"
```

Gdzie:

- "CN=Nazwa Użytkownika,OU=OU_Nazwa,DC=Nazwa_Domeny,DC=pl" to ścieżka do miejsca, gdzie chcesz dodać użytkownika.
- -samid: NazwaUzytkownika to unikalna nazwa użytkownika.
- -pwd: HasloUzytkownika to hasło użytkownika.
- -mustchpwd yes: Wymusza zmianę hasła przy następnym logowaniu.
- -memberof "CN=Nazwa Grupy,OU=OU_Nazwa,DC=Nazwa_Domeny,DC=pl" to przynależność do konkretnej grupy.

Przykład:

```
dsadd user "CN=John Doe,OU=Users,DC=example,DC=com" -samid johnd -pwd mypassword -mustchpwd yes -memberof "CN=Users,OU=Groups,DC=example,DC=com"
```

5. **Zakończ:** Po wprowadzeniu powyższego polecenia, konto użytkownika zostanie utworzone w domenie.

To zaawansowane narzędzie i wymaga dokładnej znajomości składni oraz struktury katalogu Active Directory. Wprowadzając polecenia, zachowaj ostrożność, aby uniknąć błędów, które mogą wpłynąć na funkcjonowanie kontroli domeny.

C. Wyszukiwanie grup domeny, do których należy dany użytkownik

Usługa Active Directory umożliwia elastyczne i pomysłowe zagnieżdżanie grup, przy czym:

- Grupy globalne mogą być zagnieżdżane w innych grupach globalnych, uniwersalnych lub lokalnych grupach domeny.
- Grupy uniwersalne mogą być członkami innych grup uniwersalnych lub lokalnych grup domeny.
- Lokalne grupy domeny mogą należeć do innych lokalnych grup domeny.

Elastyczność zagnieżdżania grup jest potencjalnym źródłem złożoności i bez odpowiednich narzędzi byłoby bardzo trudno dokładnie określić, do których grup należy użytkownik, czy należy bezpośrednio lub pośrednio. System Windows Server został wyposażony w polecenie DSGET, za pomocą którego można rozwiązywać takie problemy.

dsget user - wyświetla różne właściwości użytkownika w katalogu.

Przy użyciu poniższej komendy można sprawdzić, do których grup domeny należy określony użytkownik:

```
dsget user "DistinguishedNameUżytkownika" -memberof
```

W miejscu "DistinguishedNameUżytkownika" należy podać pełną nazwę odróżniającą (Distinguished Name) użytkownika, którego przynależność do grup domeny chcesz sprawdzić. Po uruchomieniu tej komendy, zostaną wyświetlone grupy, do których użytkownik jest przypisany.

Przykład:

Wydając polecenie

dsget user cn=test,ou=proba,dc=firma,dc=local -memberof -expand

otrzymaliśmy wynik, który mówi nam do jakich grup należy użytkownik test należący do jednostki organizacyjnej proba.

"CN=grproba,OU=proba,DC=FIRMA,DC=local"

"CN=Użytkownicy domeny,CN=Users,DC=Firma,DC=local"

"CN=Użytkownicy,CN=Builtin,DC=Firma,DC=local"

Przełącznik -memberof zwraca wartość atrybutu MemberOf pokazując, do których grup użytkownik należy bezpośrednio. Poprzez dodanie przełącznika -expand, grupy te będą przeszukiwane rekurencyjnie, co utworzy pełną listę wszystkich grup, do których należy dany użytkownik domeny.

D. Zarządzanie grupami. Strategie tworzenia grup

1. Strategia A L P (K L U)

Jest to najbardziej efektywna metoda nadawania określonych uprawnień do zasobów lub operacji na lokalnej maszynie wielu użytkownikom jednocześnie. Nazwa metody jest skrótem utworzonym z pierwszych liter angielskich słów "Konto" (Account), "Lokalne" (Local) i "Uprawnienia" (Permissions). W praktyce polega na dodaniu kont użytkowników lokalnych (Konta) do grupy lokalnej (Lokalne), a następnie nadaniu tej grupie określonych uprawnień (Uprawnienia).
Strategia **A L P** ma następujące zalety:

- Ułatwia zarządzanie uprawnieniami dla wielu użytkowników, ponieważ wystarczy zmienić uprawnienia dla jednej grupy, a nie dla każdego użytkownika z osobna.
- Zwiększa bezpieczeństwo systemu, ponieważ ogranicza dostęp do zasobów lub operacji tylko do tych użytkowników, którzy faktycznie go potrzebują.
- Poprawia wydajność systemu, ponieważ zmniejsza liczbę sprawdzanych uprawnień przy każdym dostępie do zasobu lub operacji.

Strategia **A L P** ma również pewne wady, takie jak:

- Może być trudna do zastosowania w środowiskach sieciowych, ponieważ wymaga synchronizacji grup i uprawnień między różnymi maszynami.
- Może być ryzykowna, jeśli nie jest odpowiednio monitorowana i aktualizowana, ponieważ może doprowadzić do nadania zbyt dużych lub zbyt małych uprawnień niektórym użytkownikom.

- Może być nieefektywna, jeśli liczba użytkowników lub zasobów jest bardzo duża lub bardzo mała, ponieważ może powodować nadmierną lub niedostateczną agregację uprawnień.

2. **Strategia A G DL P (K G DL U) - przy pojedynczej domenie**

Jest to najbardziej efektywna metoda nadawania określonych uprawnień do zasobów i operacji na maszynach należących do określonej domeny. Nazwa metody jest skrótem utworzonym z pierwszych liter angielskich słów "Konto" (Account), "Globalne" (Global), "Domenowe Lokalne" (Domain Local) i "Uprawnienia" (Permissions). Proces polega na utworzeniu kont użytkowników domenowych (Konta) i dodaniu ich do grup globalnych (Globalne), które następnie są przypisane do lokalnej grupy domenowej (Domenowe Lokalne) z odpowiednimi uprawnieniami (Uprawnienia).

Strategia **A G DL P** ma następujące zalety:

- Ułatwia implementację i zmianę uprawnień użytkowników i grup poprzez członkostwo w grupach lokalnych domenowych.
- Zmniejsza liczbę grup i członkostw grupowych w porównaniu do strategii A P.
- Jest kompatybilna ze wszystkimi domenami, nawet tymi, które nie obsługują grup uniwersalnych.

Strategia **A G DL P** ma również pewne wady, takie jak:

- Jest trudniejsza do zastosowania w środowiskach wielodomenowych i wielolasowych niż strategia A G U DL P (K G UN DL U).
- Wymaga ręcznego tworzenia i zarządzania strukturami grup w konsoli Active Directory, co jest pracochłonne i podatne na błędy.
- Nie wykorzystuje pełnego potencjału grup uniwersalnych i lasów.

3. **Strategia A G U DL P (K G UN DL U) - przy wielu domenach**

Ta strategia służy do zarządzania uprawnieniami w środowiskach z wieloma domenami. Nazwa tej strategii pochodzi od pierwszych liter angielskich słów "Konto" (Account), "Globalne" (Global), "Uniwersalne" (Universal), "Domenowe Lokalne" (Domain Local) i "Uprawnienia" (Permissions). Proces obejmuje tworzenie grup globalnych (Globalne) w każdej domenie i dodawanie do nich użytkowników z danej domeny (Konta). Następnie grupy globalne z różnych domen są agregowane w grupie uniwersalnej (Uniwersalne). Ostatecznie grupa uniwersalna jest przypisana do grupy lokalnej domenowej (Domenowe Lokalne), która określa uprawnienia (Uprawnienia) i dostęp do zasobów.

Strategia **A G U DL P (K G UN DL U)** ma wiele zalet, takich jak:

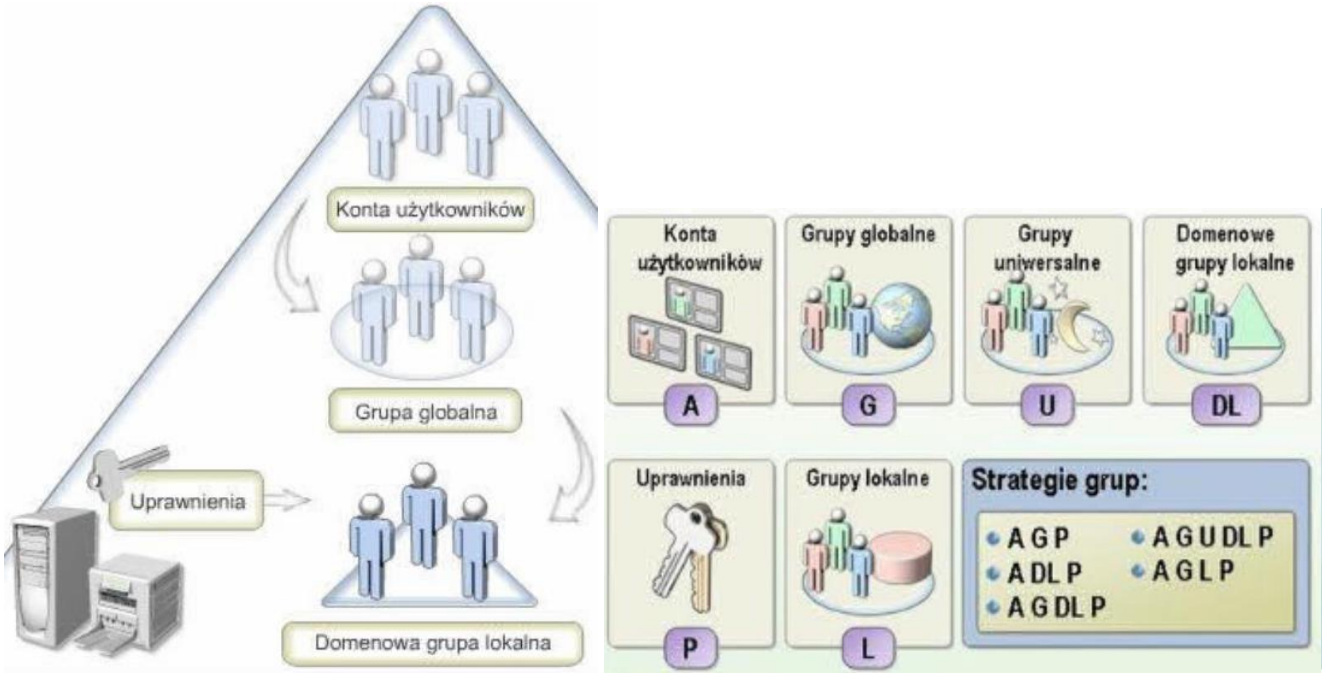
- Ułatwia zarządzanie dostępem do zasobów w różnych domenach i lasach.
- Zmniejsza liczbę grup i członkostw grupowych.
- Zapewnia większą elastyczność i skalowalność.
- Poprawia wydajność replikacji i autoryzacji.

Strategia **A G U DL P (K G UN DL U)** ma również pewne wady, takie jak:

- Jest bardziej skomplikowana do wdrożenia i utrzymania niż prostsza strategia A G DL P.
- Wymaga większej ilości uniwersalnych grup, co może wpływać na wydajność replikacji i autoryzacji.
- Nie jest kompatybilna ze starszymi domenami, które nie obsługują grup uniwersalnych.

Podsumowanie

Zarządzanie kontami użytkowników, grup oraz kontami komputerów jest niezwykle istotne dla utrzymania bezpieczeństwa i organizacji w systemach Windows. W zależności od wersji systemu operacyjnego, dostępne narzędzia i funkcje mogą się różnić, a także mogą być dodawane nowe rozwiązania, aby sprostać rosnącym wymaganiom w dziedzinie zarządzania tożsamością i dostępem.



Strategia A G DL P (K G DL U)